UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,891	08/28/2003	Ciprian Gociman	MS1-1684US	8737

22801 7590 11/04/2009

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
11/04/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/650,891	GOCIMAN, CIPRIAN	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 2, 4-13, 15-24, 26-34, and 36-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4-13, 15-24, 26-34, and 36-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on June 30, 2009. Claims 1-38 were currently pending consideration. Per the received amendment, claims 3, 14, 25, and 35 are canceled.

2. Claims 1, 2, 4-13, 15-24, 26-34, and 36-38 are currently pending consideration.

Response to Arguments

Applicant's arguments filed June 30, 2009 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Lortz (U.S. Patent 7,107,610), does not teach the newly added limitation of "the operation being associated with modification of content or functionality of the resource." This argument is not found persuasive. Lortz teaches generating resource requests which involve operations to access a file residing on a file system, print documents or some other operation (column 1, lines 45-51). Accessing a file is associated with modification of a the resource (file) because accessing a file would allow the user to possibly change, modify or delete the file. Therefore, it is asserted that the CPA does teach the operation is associated with the modification of content or functionality of the resource. Regarding the new limitation of "building an output array and logging the output array to

a log file when the request is authorized" a new reference is introduced and the arguments are moot.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 7-10, 12-14, 16, 18-20, 22-25, 27, 29-31, 33-35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lortz (U.S. Patent 7,107,610) in view of Brezak et al. (EP 1619856 A1) in further in view of Srinivasan (U.S. Patent Pub. No. US 2002/0026535).

Regarding claim 1, Lortz discloses:

A method of use by a server coupled to one or more client devices in a distributed computing environment, the method comprising:

hosting a set of resources (column 2, lines 35-41: *"resource manager"*);

receiving a request for a user to perform an operation on a resource of the resources, the request being received by an application hosted by the server (column 1, line 65 - column 2, line 9: *wherein a client generates a resource request over the network to access the resources),* and the operation being associated with modification

of content or functionality of the resource (column 1, lines 45-51*: accessing a file is associated with modification of a the resource (file) because accessing a file would allow the user to possibly change, modify or delete the file*);

determining whether to authorize the operation as a function of whether the user has been delegated administrative authority to perform the operation with respect to the resource, the administrative authority being independent of whether the user is a member of an administrators group associated with any resource of the server (column 2, lines 10-14), *wherein a client can delegate its authorization credentials to a second client which can then use those credentials to access the server.*

Lortz does not explicitly disclose that the delegated administrative authority is given by a server administrator. However, in the system of Lortz, the server authorizes a client which then can pass the credentials to another party so that the other party can access the resources controlled by the server (Lortz: column 2, lines 10-14). Brezak discloses a system wherein the server delegates authority to a client to access a resource by acting as a proxy for the client so that the client can access other resources without obtaining credentials for that particular server (Brezak: paragraphs 0031-0032, 0038-0040). It would have been obvious to use the server to assign authority to the clients, as opposed to only the clients having delegation authority as in Lortz, so that constrained delegation is provided in a controllable manner that does not require the client to forward credentials to a front-end server (Brezak: paragraph 0031).

Lortz and Brezak are silent on the limitation of building an output array and logging the output array to a log file when the request is authorized. However,

Srinivasan discloses that successful attempts of a process are output and recorded in a log file (see claim 7, paragraphs 0089, 0094, 0095). It would have been obvious to record the successful completion of a task in a log file in order to help in verifying completion and otherwise setup warnings and alerts (Srinivasan: paragraph 0047).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein determining whether to authorize the operation is performed by a secure delegation administration framework (column 2, lines 10-14), *wherein a client can delegate its authorization credentials.*

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein the request comprises a scope associated with the user, and a name of a method associated with the operation (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client.*

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein the request further comprises an indication of whether the user desires to execute the operation via a dynamically built

command line or via an executable object already associate with the operation (column 1, lines 45-52), *wherein a client is associated with a resource operation.*

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein the request further comprises an indication of whether the user desires to log a result of the operation (column 1, lines 45-52), *wherein a client is associated with a resource operation, which can include accessing a file.*

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein the secure delegation administration framework is secure at least because it does not allow the user access to mapping of user role-based permission to perform the operation directed to the resource (column 2, lines 35-43, column 3, lines 19-23), *wherein the user has no control over the mapping but the resource manager does the mapping of the resource requests.*

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein the method further comprises:

installing the application on the server (column 2, lines 35-37), *wherein a resource manager is a program module installed on the server*;

responsive to the installing, the application identifying a set of operations that the application can perform (column 2, lines 15-19, 51-56), *wherein the resources that a server manages is determined*;

mapping, by a member of the administrators group, the operations to a set of security permissions based on authorization specific role(s) of a set of users comprising the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization credentials which represent the privilege level that the client is assigned;* and

wherein determining further comprises the application utilizing the mapping to identify whether the user has permission to perform the operation (column 2, lines 35-50), *wherein the authorization credentials accompanying the resource request are mapped to a certain access level, so that the server can check if the client is authorized to access the requested resource.*

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Lortz discloses:

A method as recited in claim 1, wherein responsive to determining that the user has been delegated authority to perform the operation with respect to the resource, the method further comprises:

setting parameters associated with the operation (column 1, lines 45-50); and

executing the operation within a scope associate with the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization credentials which represent the privilege level that the client is assigned in regards to the resource.*

Regarding claim 13, Lortz discloses:

A computer-readable medium for use in a distributed computing environment including a server and one or more client computing devices coupled to the server, the computer-readable medium comprising computer-executable instructions than, when executed, cause one or more processors to perform acts including :

hosting a set of resources(column 2, lines 35-41: "*resource manager*"), a particular resource of the resources allowing a user to determine whether the user has delegated authority to access a resource of the resources (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client* and the operation being associated with modification of content or functionality of the resource (column 1, lines 45-51*: accessing a file is associated with modification of a the resource (file) because accessing a file would allow the user to possibly change, modify or delete the file*);

receiving a request from the user to perform an operation on the resource (column 1, line 65 - column 2, line 9), *wherein a client generates a resource request over the network to access the resources*; and

determining whether to authorize the operation as a function of whether the user has been delegated a role-based scope of authority to perform the operation, the role-

based scope of authority not requiring the user to be a member of an administrators group associated with any resources of the server (column 2, lines 10-14), *wherein a client can delegate its authorization credentials to a second client which can then use those credentials to access the server.*

Lortz does not explicitly disclose that the delegated administrative authority is given by a server administrator. However, in the system of Lortz, the server authorizes a client which then can pass the credentials to another party so that the other party can access the resources controlled by the server (Lortz: column 2, lines 10-14). Brezak discloses a system wherein the server delegates authority to a client to access a resource by acting as a proxy for the client so that the client can access other resources without obtaining credentials for that particular server (Brezak: paragraphs 0031-0032, 0038-0040). It would have been obvious to use the server to assign authority to the clients, as opposed to only the clients having delegation authority as in Lortz, so that constrained delegation is provided in a controllable manner that does not require the client to forward credentials to a front-end server (Brezak: paragraph 0031).

Lortz and Brezak are silent on the limitation of building an output array and logging the output array to a log file when the request is authorized. However, Srinivasan discloses that successful attempts of a process are output and recorded in a log file (see claim 7, paragraphs 0089, 0094, 0095). It would have been obvious to record the successful completion of a task in a log file in order to help in verifying completion and otherwise setup warnings and alerts (Srinivasan: paragraph 0047).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Lortz discloses:

A computer-readable medium as recited in claim 13, wherein the operation is associated with modification of content and/or functionality of the resource (column 1, lines 45-52), *wherein the client is associated with a resource operation.*

Claim 16 is rejected as applied above in rejecting claim 13. Furthermore, Lortz discloses:

A computer-readable medium as recited in claim 13, wherein the request comprises a scope associated with the user, and a name of a method associated with the operation (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client.*

Claim 18 is rejected as applied above in rejecting claim 13. Furthermore, Lortz discloses:

A computer-readable medium as recited in claim 13, wherein the request further comprises an indication of whether the operation is to be executed via a dynamically built command line or via an executable object already associated with the operation (column 1, lines 45-52), *wherein a client is associated with a resource operation.*

Claim 19 is rejected as applied above in rejecting claim 13. Furthermore, Lortz discloses:

A computer-readable medium as recited in claim 13, wherein operations associated with determining whether to authorize the operations are secure at least because the user does not have access to user role-based permission(s) to perform the operation (column 2, lines 35-43, column 3, lines 19-23), *wherein the user has no control over the mapping but the resource manager does the mapping of the resource requests.*

Claim 20 is rejected as applied above in rejecting claim 13. Furthermore, Lortz discloses:

A computer-readable medium as recited in claim 13, wherein the computer-executable instructions comprise instructions that cause the one or more processors to perform acts further including:

identifying a set of operations associated with the resource (column 2, lines 15-19, 51-56), *wherein the resources that a server manages is determined*;

mapping the operations to a set of security permissions, the security permissions being based on authorization specific role(s) of a set of users comprising the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization credentials which represent the privilege level that the client is assigned*; and

wherein the instructions for determining further comprise instructions for utilizing the mapping to identify whether the user has permission to perform the operation

(column 2, lines 35-50), *wherein the authorization credentials accompanying the resource request are mapped to a certain access level, so that the server can check if the client is authorized to access the requested resource.*

Claim 22 is rejected as applied above in rejecting claim 13. Furthermore, Lortz discloses:

A computer-readable medium as recited in claim 13, wherein the computer-executable instructions, responsive to determining that the user has been delegated authority to perform the operation with respect to the resource, comprise instructions that cause the one or more processors to perform acts further including:

setting parameters associated with the operation (column 1, lines 45-50); and

executing the operation within a scope associated with the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization credentials which represent the privilege level that the client is assigned in regards to the resource.*

Regarding claim 23, Lortz discloses:

A server for use in a distributed computing environment including the server and one or more client computing devices coupled to the server, the server comprising:

one or more processors (column 2, lines 35-41: *"resource manager"*);; and

a memory coupled to the one or more processors, the memory comprising computer-executable instructions that cause the one or more processors to perform acts including:

hosting a set of resources(column 2, lines 35-41: "*resource manager*");;

receiving a request from a user to perform an operation on a resource of the resources (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client* and the operation being associated with modification of content or functionality of the resource (column 1, lines 45-51*: accessing a file is associated with modification of a the resource (file) because accessing a file would allow the user to possibly change, modify or delete the file*); and

determining whether to authorize the operation as a function of whether the user has been delegated a role-based scope of authority to perform the operation, the role-based scope of authority not requiring the user to be a member of an administrators group associated with resources of the server (column 2, lines 10-14), *wherein a client can delegate its authorization credentials to a second client which can then use those credentials to access the server.*

Lortz does not explicitly disclose that the delegated administrative authority is given by a server administrator. However, in the system of Lortz, the server authorizes a client which then can pass the credentials to another party so that the other party can access the resources controlled by the server (Lortz: column 2, lines 10-14). Brezak discloses a system wherein the server delegates authority to a client to access a resource by acting as a proxy for the client so that the client can access other resources without obtaining credentials for that particular server (Brezak: paragraphs 0031-0032, 0038-0040). It would have been obvious to use the server to assign authority to the clients, as opposed to only the clients having delegation authority as in Lortz, so that

constrained delegation is provided in a controllable manner that does not require the client to forward credentials to a front-end server (Brezak: paragraph 0031).

Lortz and Brezak are silent on the limitation of building an output array and logging the output array to a log file when the request is authorized. However, Srinivasan discloses that successful attempts of a process are output and recorded in a log file (see claim 7, paragraphs 0089, 0094, 0095). It would have been obvious to record the successful completion of a task in a log file in order to help in verifying completion and otherwise setup warnings and alerts (Srinivasan: paragraph 0047).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Lortz discloses:

A server as recited in claim 23, wherein the request is generated by at least one resource of the resources (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client.*

Claim 27 is rejected as applied above in rejecting claim 23. Furthermore, Lortz discloses:

A server as recited in claim 23, wherein the request comprises a scope associated with the user, a name of a method associated with the operation (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client.*

Claim 29 is rejected as applied above in rejecting claim 23. Furthermore, Lortz discloses:

A server as recited in claim 23, wherein the request further comprises an indication of whether the operation is to be executed via a dynamically built command line or via an executable object already associated with the operation (column 1, lines 45-52), *wherein a client is associated with a resource operation.*

Claim 30 is rejected as applied above in rejecting claim 23. Furthermore, Lortz discloses:

A server as recited in claim 23, wherein the secure delegation administration framework is secure at least because it does not allow the user access to a mapping of user role-based permission to perform the operation directed to the resource (column 2, lines 35-43, column 3, lines 19-23), *wherein the user has no control over the mapping but the resource manager does the mapping of the resource requests.*

Claim 31 is rejected as applied above in rejecting claim 23. Furthermore, Lortz discloses:

A server as recited in claim 23, wherein the computer-executable instructions further comprise instructions that cause the one or more processors to perform acts further including:

identifying a set of operations associated with the resource (column 2, lines 15-19, 51-56), *wherein the resources that a server manages is determined*;

mapping the operations to a set of security permissions based on authorization specific role(s) of a set of users comprising the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization credentials which represent the privilege level that the client is assigned*; and

wherein the instructions for determining further comprise instructions for utilizing the mapping to identify whether the user has permission to perform the operation column 2, lines 35-50), *wherein the authorization credentials accompanying the resource request are mapped to a certain access level, so that the server can check if the client is authorized to access the requested resource*.

Claim 33 is rejected as applied above in rejecting claim 23. Furthermore, Lortz discloses:

A server as recited in claim 23, wherein the computer-executable instructions, responsive to determining that the user has been delegated authority to perform the operation with respect to the resource, further comprise instructions that cause the one or more processors to perform acts further including:

setting parameters associated with the operation (column 1, lines 45-50); and

executing the operation within a scope associated with the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization credentials which represent the privilege level that the client is assigned in regards to the resource*.

Regarding claim 34, Lortz discloses:

A server comprising:

means for hosting a set of resources (column 2, lines 35-41: *"resource manager"*);

means for receiving a request from the user to perform an operation on a resource of the resources (column 1, line 65 - column 2, line 9), *wherein a client generates a resource request over the network to access the resources* and the operation being associated with modification of content or functionality of the resource (column 1, lines 45-51*: accessing a file is associated with modification of a the resource (file) because accessing a file would allow the user to possibly change, modify or delete the file*); and

means for determining whether to authorize the operation as a function of whether the user has been delegated a role-based scope of authority to perform the operation, the role-based scope of authority not requiring the user to be a member of an administrators group associated with the server (column 2, lines 10-14), *wherein a client can delegate its authorization credentials to a second client which can then use those credentials to access the server.*

Lortz does not explicitly disclose that the delegated administrative authority is given by a server administrator. However, in the system of Lortz, the server authorizes a client which then can pass the credentials to another party so that the other party can access the resources controlled by the server (Lortz: column 2, lines 10-14). Brezak discloses a system wherein the server delegates authority to a client to access a resource by acting as a proxy for the client so that the client can access other resources

without obtaining credentials for that particular server (Brezak: paragraphs 0031-0032, 0038-0040). It would have been obvious to use the server to assign authority to the clients, as opposed to only the clients having delegation authority as in Lortz, so that constrained delegation is provided in a controllable manner that does not require the client to forward credentials to a front-end server (Brezak: paragraph 0031).

Lortz and Brezak are silent on the limitation of building an output array and logging the output array to a log file when the request is authorized. However, Srinivasan discloses that successful attempts of a process are output and recorded in a log file (see claim 7, paragraphs 0089, 0094, 0095). It would have been obvious to record the successful completion of a task in a log file in order to help in verifying completion and otherwise setup warnings and alerts (Srinivasan: paragraph 0047).

Claim 38 is rejected as applied above in rejecting claim 34. Furthermore, Lortz discloses:

A server as recited in claim 34, wherein responsive to determining that the user has been delegated authority to perform the operation with respect to the resource, the server further comprises:

means for setting parameters associated with the operation (column 1, lines 45-50); and

means for executing the operation within a scope associated with the user (column 1, lines 39-44), *wherein each client is associated (mapped) to authorization*

credentials which represent the privilege level that the client is assigned in regards to the resource.

Claims 6,11,15,17,21,26,28,32 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lortz (U.S. Patent 7,107,610) in view of Brezak et al. (EP 1619856 A1) further in view of Srinivasan (U.S. Patent Pub. No. US 2002/0026535) in further in view of Krishnan et al. (U.S. Patent 6,222,856).

Claims 4, 15, 26, and 36 are rejected as applied above in rejecting the claims above. Lortz-Brezak-Srinivasan does not explicitly teach that the resource is an Internet Information Service (IIS) metabase node. Krishnan discloses a IIS system which uses a metabase to obtain information about any virtual service (Krishnan: column 6, lines 37-46). Lortz-Brezak-Srinivasan and Krishnan are analogous arts because both have to do with controlling resources via a server. It would have been obvious to use the IIS metabase of Krishnan in the resource authorization framework of Lortz-Brezak-Srinivasan so the authorization framework of Lortz can use the metabase of Krishnan to look up names of virtual services, and their bandwidth thresholds, so that it can more efficiently authorize requests and reduce network congestion (Krishnan: column 6, lines 35-47).

Claims 6, 17, 28, and 37 are rejected as applied above in rejecting the claims above.). Lortz-Brezak-Srinivasan teaches a server and that a client cannot perform

administrative activities associated with the server without sending a request to the server for permission evaluation (Lortz: column 1, line 65 - column 2, line 9). Lortz does not explicitly teach that the resources that are to be accessed are Web sites hosted by an ISP. Krishnan discloses that a network server is an ISP that provides services to a client over the Internet (Krishnan: column 4, lines 23-37). It would have been obvious for the network server of Lortz-Brezak to be an ISP hosting Web sites, as the system of Lortz is over the Internet, and ISPs are ubiquitous throughout the Internet.

Claims 11, 21, and 32 are rejected as applied in rejecting the claims above. Furthermore, Lortz discloses:

specifying, by a member of a administrators group, role-based user access permissions to nodes (column 2, lines 35-50), *wherein the authorization credentials accompanying the resource request are mapped to a certain access level, so that the server can check if the client is authorized to access the requested resource*;

indicating an interface to a task, the interface comprising a set of parameters and a name (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client*, the task comprising the operation; and

wherein determining further comprises:

locating the interface in a configuration file (column 2, lines 45-50), *wherein the service searches the resource structure to find the client's information (configuration file) to check if the client's request should be granted*;

responsive to locating the interface, presenting an identity of the user to the resource to evaluate a scope in view of the parameters and the name of the resource (column 1, line 65 – column 2, line 9), *wherein the resource request includes the authorization credentials for the client*; and

responsive to the presenting, identifying whether the user has been delegated a role-based access permission to perform the operation with respect to the resource server (column 2, lines 10-14), *wherein a client can delegate its authorization credentials to a second client which can then use those credentials to access the server.*

Lortz-Brezak-Srinivasan does not explicitly teach that the resource is an Internet Information Service (IIS) metabase node. Krishnan discloses a IIS system which uses a metabase to obtain information about any virtual service (Krishnan: column 6, lines 37-46). Lortz and Krishnan are analogous arts because both have to do with controlling resources via a server. It would have been obvious to use the IIS metabase of Krishnan in the resource authorization framework of Lortz-Brezak so the authorization framework of Lortz can use the metabase of Krishnan to look up names of virtual services, and their bandwidth thresholds, so that it can more efficiently authorize requests and reduce network congestion (Krishnan: column 6, lines 35-47).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
10/29/2009
Primary Examiner, Art Unit 2431